Data Protection Policy

Introduction

This policy reflects the new General Data Protection Regulation (GDPR) which came into force on 25 May 2018. All IOSH staff are always required to adhere to this policy.

Purpose

IOSH, for the purposes of this policy, includes both the Institution of Occupational Safety and Health (Registration Number: Z5637476) and its subsidiary IOSH Services Limited (Registration Number: Z5637522). Both are data controllers registered with the Information Commissioner's Office (ICO) in accordance with the GDPR. IOSH holds and processes personal data for the purposes notified to the ICO, whose register of data controllers is open to public inspection via its website (www.ico.gov.uk).

These purposes enable IOSH to:

- pursue the objectives in its Royal Charter (under which it acts in the public interest),
- fulfil contractual obligations, and
- operate as efficiently as possible.

IOSH will communicate those purposes to each individual when their personal data is gathered and will not disclose that personal data for other purposes unless required to do so to comply with GDPR.

Individuals who process or use any personal data on behalf of IOSH must also comply with the GDPR. IOSH may, from time to time, be required to share personal information about members with other organizations, to facilitate delivery of our services to them or to comply with our legal obligation. We never sell members' personal data or share it unnecessarily.

This policy applies to anyone working with personal data that is controlled or processed by or on behalf of IOSH including, but not limited to, staff, trustees and council members. It ensures that all are aware of their responsibilities and outlines how IOSH complies with the following core principles of the GDPR.

Organisational methods for keeping data secure are imperative, IOSH believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy complies with the requirements set out in the GDPR and other relevant legislation.

Scope

This policy has due regard to legislation including, but not limited to, the following:

- the General Data Protection Regulation (GDPR)
- UK Parliament data protection legislation and draft legislation
- The Human Rights Act 1998

This policy has regard to the Information Commissioner's Office guidance on best practice.

Applicable data

Personal data

- This refers to information that relates to an identifiable, living individual, including information such as an online identifier, for example an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded data.

Special categories of personal data

- Sensitive personal data is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

Personal data relating to criminal convictions and offences

- For our lawful processing purposes this means data relating to unspent criminal convictions or cautions.

Principles

In accordance with the requirements outlined in the GDPR, personal data will be:

- processed lawfully, fairly and in a transparent manner.
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes.
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

"The controller" shall be responsible for, and able to demonstrate, compliance with the principles set out above.

Implementing the principles

IOSH will:

- establish and maintain appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in this policy and related legislation.
- provide comprehensive, clear and transparent privacy policies.
- maintain records of activities relating to higher-risk processing activities.
- ensure internal records of processing activities include the following:
  - name and details of the organisation
  - purpose(s) of the processing

- description of the categories of individuals and personal data
- retention schedules
- categories of recipients of personal data
- description of technical and organisational security measures.

Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place, adopt privacy-by-design principles such as:

- data minimisation
- pseudonymisation
- transparency
- allowing individuals to monitor processing
- continuously creating and improving security features
- use of data protection impact assessments, where appropriate

Data protection officer (DPO)

The Information Security Officer, will undertake the role of DPO for IOSH and will:

- inform and advise IOSH and its employees about their obligations to comply with the GDPR and other data protection laws.
- monitor IOSH's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits and providing the required training to staff members.

The DPO will have professional experience and knowledge of data protection law, particularly in relation to trusts.

The DPO will report to the Chief Executive Officer, but will operate independently and will not be dismissed or penalised for performing their task. Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

Lawful processing

The legal basis for processing data will be identified and documented prior to data being processed. Under the GDPR, data will be lawfully processed under the following conditions.

- The consent of the data subject has been explicitly obtained

  or where

- Processing is necessary for:
  - compliance with a legal obligation.
  - the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
  - the performance of a contract with the data subject or to take steps to enter into a contract.
  - protecting the vital interests of a data subject or another person.
  - the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Special Category and Criminal Conviction and Offences data will only be processed under the following conditions.

- Explicit consent of the data subject unless reliance on consent is prohibited by EU or Member State law.

  Or where

- Processing is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
    - carrying out obligations under employment, social security or social protection law, or a collective agreement.
    - protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
    - archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

Consent

Where it is agreed that consent is needed, it must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

Where consent is given, a record will be kept documenting how and when consent was given.

IOSH ensures that consent mechanisms meet the standards of the GDPR.

Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR. However, acceptable consent obtained under the DPA will not be reobtained.

Consent can be withdrawn by the individual at any time.

The right to be informed

In relation to data, obtained both directly from the data subject and received from third parties, the following information will be supplied in the privacy notice.

- The identity and contact details of the controller, and where applicable, the controller's representative and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
    - withdraw consent at any time.
    - lodge a complaint with a supervisory authority.
- The existence of automated decision-making, including profiling, and information on how decisions are made, the significance of the process and the consequences.

Where data are obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

Where data are not obtained directly from the data subject, information regarding the source the personal data originates from, and whether it came from publicly accessible sources, will be provided.

For data obtained directly from the data subject, this information will be supplied at the time the data are obtained.

In relation to data that are not obtained directly from the data subject, this information will be supplied:

- within 30 days of having obtained the data.
- if disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- if the data are used to communicate with the individual, at the latest, when the first communication takes place.

The right of access

Individuals have the right to obtain confirmation that their data are being processed.

Individuals have the right to submit a subject access request (SAR) to gain access to their personal data to verify the lawfulness of the processing. The SAR procedure can be found on the IOSH Information Security page of the Intranet and via the IOSH website.

IOSH will verify the identity of the person making the request before any information is supplied. A copy of the information will be supplied to the individual free of charge. However, IOSH may impose a 'reasonable fee' to comply with requests for further copies of the same information. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee may be charged. All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and, at the latest, within one month of receipt.

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, IOSH holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal. If a large quantity of information is being processed about an individual, they will be asked to clarify their request.

The right to rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified. Where the personal data in question have been disclosed to third parties, IOSH will inform them of the rectification where possible.

Where appropriate, IOSH will inform the individual about the third parties to whom the data has been disclosed.

Requests for rectification will be responded to within 30 days; this will be extended by two months where the request for rectification is complex.

Where no action is being taken in response to a request for rectification, IOSH will explain the reason for this to the individual and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The right to erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

- where the personal data are no longer necessary in relation to the purpose for which they were originally collected or processed
- when the individual withdraws their consent
- when the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- the personal data were unlawfully processed
- the personal data are required to be erased to comply with a legal obligation
- the personal data are processed in relation to the offer of information society services to a child.

IOSH has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- to exercise the right of freedom of expression and information
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority
- for archiving purposes in the public interest, scientific research, historical research or statistical purposes
- the exercise or defence of legal claims

Where personal data have been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data have been made public in an online environment, IOSH will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

The right to restrict processing

Individuals have the right to block or suppress IOSH's processing of personal data.

If processing is restricted IOSH will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

IOSH will restrict the processing of personal data in the following circumstances:

- where an individual contests the accuracy of the personal data, processing will be restricted until IOSH has verified the accuracy of the data
- where an individual has objected to the processing and IOSH is considering whether its legitimate grounds override those of the individual
- where processing is unlawful, and the individual opposes erasure and requests restriction instead

- where IOSH no longer needs the personal data, but the individual requires the data to establish, exercise or defend a legal claim.

If the personal data in question has been disclosed to third parties, IOSH will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

IOSH will inform individuals when a restriction on processing has been lifted.

The right to data portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services. IOSH will ensure that personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- to personal data that an individual has provided to a controller
- where the processing is based on the individual's consent or for the performance of a contract
- when processing is carried out by automated means.

Personal data will be provided in a structured, commonly used and machine-readable form. IOSH will provide the information free of charge.

Where feasible, data will be transmitted directly to another organisation at the request of the individual.

IOSH is not required to adopt or maintain processing systems which are technically compatible with other organisations.

If the personal data concern more than one individual, IOSH will consider whether providing the information would prejudice the rights of any other individual.

IOSH will respond to any requests for portability within 30 days.

Where the request is complex, or several requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, IOSH will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The right to object

IOSH will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

- processing based on legitimate interests or the performance of a task in the public interest
- direct marketing
- processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

- an individual's grounds for objecting must relate to his or her situation.
- IOSH will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where IOSH can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- IOSH will stop processing personal data for direct marketing purposes as soon as an objection is received
- IOSH cannot refuse an individual's objection regarding data that are being processed for direct marketing purposes.

Where personal data are processed for research purposes:

- the individual must have grounds relating to their situation to exercise their right to object
- where the processing of personal data is necessary for the performance of a public interest task, IOSH is not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above, but is carried out online, IOSH will offer a method for individuals to object online.

Privacy by design and privacy impact assessments

IOSH will adopt a privacy-by-design approach and implement technical and organisational measures which demonstrate how IOSH has considered and integrated data protection into processing activities.

Data protection impact assessments (DPIAs) will be the responsibility of the DPO and will be incorporated into our Change Management Process where applicable. It will be used to identify the most effective method of complying with IOSH's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow IOSH to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to IOSH's reputation which might otherwise occur. A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

A DPIA will be used for more than one project, where necessary. High-risk processing includes, but is not limited to, the following:

- systematic and extensive processing activities, such as profiling
- large-scale processing of special categories of data or personal data which are in relation to criminal convictions or offences.

IOSH will ensure that all DPIAs include the following information:

- a description of the processing operations and the purposes
- an assessment of the necessity and proportionality of the processing in relation to the purpose
- an outline of the risks to individuals
- the measures implemented to address risk.

Where a DPIA indicates high-risk data processing, IOSH will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

Data breaches

The term ‘personal data breach’ refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

- The Data Protection Officer will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their continuous development training.
- Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.
- All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of IOSH becoming aware of it.
- The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.
- If a breach is likely to result in a high risk to the rights and freedoms of an individual, IOSH will notify those concerned directly.
- A ‘high-risk’ breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.
- If a breach is sufficiently serious, the public will be notified without undue delay.

Effective and robust breach detection, investigation and internal reporting procedures are in place at IOSH, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

Within a breach notification, the following information will be outlined:

- the nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- the name and contact details of the DPO
- an explanation of the likely consequences of the personal data breach
- a description of the proposed measures to be taken to deal with the personal data breach
- where appropriate, a description of the measures taken to mitigate any possible adverse effects.

Failure to report a breach when required to do so will result in a fine, as well as a fine for the breach itself.

The IOSH Data Breach Policy and Procedure can be found on the Information Security page of the IOSH Intranet.

Data security

- Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.
- Confidential paper records will not be left unattended or in clear view anywhere with general access.
- Electronic data will be digitally encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.
- Where data are saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.
- Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.
- All electronic devices are password-protected to ensure the security of the information on the device in case of theft.
- Staff will not use their personal laptops or computers for IOSH purposes.
- All relevant members of staff are provided with their own secure log-in and password, and every computer prompts users to change their password every six months.
- Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from IOSH premises accepts full responsibility for the security of the data.

Before sharing data, all staff members will ensure:

- they can share it.
- adequate security is in place to protect it.
- a privacy notice has outlined who will receive the data.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of IOSH containing sensitive information are always supervised.

The physical security of IOSH's buildings and storage systems, and access to them, is reviewed on a yearly basis. If an increased risk in vandalism, burglary and theft is identified, extra measures to secure data storage will be put in place.

IOSH takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

The Data Protection Officer is responsible for ensuring continuity and recovery measures are in place to ensure the security of protected data.

Publication of information

IOSH will not publish any personal information, including photos, on its website without the permission of the affected individual.

When uploading information to the IOSH website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

CCTV and photography

IOSH understands that recording images of identifiable individuals constitutes processing personal information, so it is done in accordance with the GDPR.

IOSH does not capture CCTV images.

IOSH will always indicate its intentions for taking photographs of staff and visitors to The Grange and will retrieve permission before publishing them.

Images captured by individuals for recreational or personal purposes, and videos made by staff for family use, are exempt from the GDPR.

Data retention

Data will not be kept for longer than necessary. Unrequired data will be deleted as soon as practicable.

IOSH has a data retention & archive policy which details what data are kept and how long they should be kept for. Please refer to the Data Retention & Archive Policy which can be found on the Information Security page of the IOSH Intranet site and also the IOSH website.

Paper documents will be shredded or put into confidential waste for secure disposal.

Confirmation

This Policy is part of the induction process for new starters to IOSH and existing staff will be reminded of the policy on a yearly basis.

By confirming you have read this document you agree to abide by the Data Protection Policy for the duration of your employment with IOSH.

Review

This policy is subject to review as part of the annual review by the Data Protection Office.

Version control

V	Last amended	Author	Reason for amendment	Review date
1	25.05.18	LM	GDPR	25.05.19
1.1	12.06.18	LM	Text amends	12.06.19
1.3	30.09.20	LM	GDPR Audit Recommendations	30.09.20

Policy document information

Policy owner	Information Security Officer	**Policy contact**	Laura Mills
Purpose	To provide staff and workers with clear guidance on IOSH Data Protection		
Related operational policies	Reference is made to supplementary procedures including the Subject Access Request procedure, Data Breach Procedure, Data Retention & Archive Policy. These documents can be found on the Information Security page of the IOSH Intranet.		
Relevant committees	GDPR working group		
Relevant legislation and standards	Data Protection Act 1998, GDPR, ISO 27001		
Communication plan	Central Electronic Repository Communications programme awareness to all staff		
Distribution	All staff	**Introduced**	04.06.2018
Review period	Annual	**Sign-off**	Accountable – Director of Transformation and Technology (JOD) Responsible – Information Security Officer (LM) Consulted – BMG/IT Management Informed – Staff, members, volunteers and workers

Reference to other policies/business rules/processes/forms

Document Name	Location